UNIVERSITE MOHAMMED V
FACULTE DES SCIENCES

ANNEE UNIVERSITAIRE 2017-2018
Master APQ

EXAMEN
CRYPTOGRAPHIE CLASSIQUE
DUREE : 2H

Questions de cours (2.5pt)
Donner la définition technique des termes suivants : **Confidentialité, Disponibilité, Intégrité, Authentification, Non-répudiation.**

Exercice 1 (2.5pt)
On utilisant le cryptosystème de **Vigenère** crypter la phrase suivante : **« Bonjour le monde »** sachant que la clé **K= {2, 6,7}.**
Rappelons que :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Exercice 2 (3pt)
Crypter le mot " **master**" en utilisant le chiffrement de Hill, sachant que la clé $K = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$.

Exercice 3 (8pt)
On considère la clé suivante :
K= 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001
a. Le DES se base sur quelle schéma? **(0.5pt)**
b. Donner la taille de **K** en bit ? **(0.5pt)**
c. Créer les 16 sous-clés nécessaires pour le chiffrement d'un texte avec le **DES. (7pt)**

Rappelons que :
Permutation initiale 1

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Décalage dans la création des sous-clés

Rond (round)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
nombre	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Exercice 4 (4pt)
Alice veux envoyer un message a Bob en utilisant le cryptosystème RSA pour crypter le texte.
Supposons qu'Alice a choisi deux nombres premiers $p = 5$ et $q = 17$ *et un exposant* $e = 5$.
a. Calculer la clé publique. **(1pt)**
b. Calculer la clé privée. **(3pt)**